Source:
tynmagazine

Pocas empresas argumentarían que sus sistemas de TI no se beneficiarían de medidas de seguridad adicionales. Particularmente en América Latina, considerando el aumento de ciberataques en la región, que representó el 9% del total de ataques observados por IBM Security X-Force en 2020, frente al 5% en 2019.

La pregunta en torno a las mejoras de seguridad, en particular el cifrado, siempre ha sido: ¿a qué costo?

No solo el costo en términos del dinero necesario para desarrollar o implementar una mejor seguridad y contratar personal capaz de administrar el cifrado y otras tecnologías complejas, sino también el impacto de tales medidas en el rendimiento de la red y las aplicaciones.

Los esfuerzos para reducir dichos costos se han cumplido con éxito en los últimos años, y las innovaciones en el horizonte pronto ofrecerán a las organizaciones mejores formas de protegerse de las amenazas de ciberseguridad tanto actuales como emergentes:

Computación Confidencial

La computación confidencial proporciona garantías de privacidad a nivel de hardware al cifrar los datos dentro de un enclave seguro que ni siquiera el proveedor de la nube puede ver o acceder.
Piense en la computación confidencial como una caja fuerte en la habitación de un hotel. La habitación del hotel es un espacio privado dentro de un edificio donde se hospedan otras personas, en el que puede esperar cierto nivel de privacidad para realizar sus actividades y guardar sus pertenencias cuando se vaya por el día. Por supuesto, el personal del hotel aún puede acceder a la habitación, por lo que confía en que no violarán su privacidad.

Las pertenencias que requieren seguridad adicional se guardan en la caja fuerte de la habitación, para lo cual solo usted conoce el código. De esta manera, incluso si el personal del hotel debe ingresar a la habitación para limpiar, no puede acceder a esas posesiones más valiosas.

En 2018, IBM se convirtió en el primer proveedor de nube en ofrecer computación confidencial para su uso en producción. Hoy, IBM ofrece capacidades de computación confidencial a través de IBM Cloud Hyper Protect Services, y está integrado en el IBM Cloud for Financial Services.

Criptografía cuántica segura

A pesar de los muy esperados beneficios de la computación cuántica, la capacidad superior de la tecnología para factorizar grandes números tiene a muchas personas preocupadas por la seguridad de los enfoques

actuales de la criptografía a medida que la computación cuántica madura.

Reconociendo esas preocupaciones, IBM Research, el Instituto Nacional de Estándares y Tecnología (NIST) y la comunidad de criptografía en general han explorado durante los últimos años nuevos enfoques para el cifrado y la protección de datos para mantener los datos confidenciales a salvo de las computadoras cuánticas. Una preocupación es que alguien pueda robar datos cifrados y retenerlos hasta que la computación cuántica avance lo suficiente como para descifrar los estándares de cifrado actuales.

La buena noticia: los investigadores están desarrollando criptografía cuántica segura para contrarrestar los esfuerzos por descifrar datos cifrados utilizando computadoras cuánticas.

IBM anunció en noviembre de 2020 soporte de criptografía cuántica segura para la gestión de claves y transacciones de aplicaciones en IBM Cloud. Además, IBM Cloud también está introduciendo soporte de criptografía cuántica segura para permitir transacciones de aplicaciones. Cuando las aplicaciones en contenedores nativas de la nube se ejecutan en Red Hat OpenShift on IBM Cloud o IBM Cloud Kubernetes Services, las conexiones de la capa de transporte seguras pueden ayudar a las transacciones de aplicaciones con soporte de criptografía cuántica segura durante el tránsito de datos.

Criptografía totalmente homomórfica

La Criptografía totalmente homomórfica (Fully Homomorphic Encryption – FHE) permite que los datos permanezcan cifrados durante la computación, independientemente de la nube o la infraestructura utilizada para procesarlos. Como resultado, FHE podría ayudar a impulsar una mayor adopción de arquitecturas de nube híbrida, permitiendo que los datos se muevan entre las nubes sin comprometer la seguridad.

FHE se basa en un algoritmo matemático diferente al cifrado tradicional, diseñado para que los cálculos se puedan realizar directamente en datos encriptados. Este modelo de cifrado emergente podría permitir que terceros procesen y analicen datos cifrados de salud, financieros o de otro tipo en la nube y devuelva resultados precisos al propietario de los datos, sin tener que exponer los datos originales en texto sin formato.

Mientras que FHE hace solo unos años requería cientos de líneas de código y horas para procesar, los investigadores anunciaron que ahora se puede ejecutar como una llamada API a la nube con 12 líneas de código en fracciones de segundo. IBM está ayudando a llevar FHE del ámbito de la investigación a la adopción temprana con los clientes, publicando kits de herramientas de código abierto para desarrolladores, y en diciembre IBM Security lanzó sus servicios de Homomorphic Encryption para que los clientes comiencen a experimentar con la tecnología.

Disponible en:
https://www.tynmagazine.com/la-seguridad-primero-3-avances-clave-para-el... [1]

Links
[1] https://www.tynmagazine.com/la-seguridad-primero-3-avances-clave-para-el-futuro-de-la-criptografia/